C. P. Bartholomew (State Bar No. 211425)
cpbartholomew@finkelsteinthompson.com
Mark Punzalan (State Bar No. 247599)
mpunzalan@finkelsteinthompson.com
FINKELSTEIN THOMPSON LLP
100 Bush Street, Suite 1450
San Francisco, CA 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

[Additional Counsel Listed on Signature Page]

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SC

CV 07 5739

JOEL RUIZ, On Behalf of Himself and All Others Similarly Situated,

Plaintiff,

vs.

GAP, INC., and DOES 1-9 inclusive,

Defendants.

COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiff Joel Ruiz ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following against the above-captioned Defendants, based upon personal knowledge, where applicable, and on information and belief and the investigation and research of counsel:

PARTIES

1. Plaintiff Joel Ruiz ("Plaintiff") is a citizen of the State of Texas. Plaintiff has been injured as a result of the unlawful conduct herein.

2. Defendant Gap Inc. ("Gap" or the "Company") is a clothing and accessories retailer based in San Francisco, California. Gap operates stores under its various brands, including Old Navy, Banana Republic, and Piperlime. Gap is headquartered at Two Folsom Street, San Francisco, California 94105.

3. Defendants DOES 1-9 are unidentified third party vendors that collect and manage Gap's job applicant information. Plaintiff does not know the identities or locations of DOES 1-9 at this time. Plaintiff will amend his complaint when he learns the identities or locations of DOES 1-9.

NATURE OF ACTION

4. Gap is a clothing and accessories dealer that has more than 154,000 employees and more than 3,100 stores in the world. Thousands of people apply for positions at Gap brand stores each year.

5. On Friday, September 28, 2007, Gap disclosed that two laptop computers with the personal information of approximately 800,000 job applicants had been stolen from one of its recruiting vendors. This personal information is readily accessible to anyone with possession because it was not encrypted.

6. Plaintiff applied for a position online with one of Gap's brand store, Old Navy, through the Gap website. As part of the application, Plaintiff was required to provide his personal information which included his social security number. Plaintiff's social security number and other personal information were entrusted to Gap and said information, on information and belief, were contained on the stolen laptops.

7. The data on the laptop computers included the names, social security numbers, addresses, and other personal information and identities of people from the United States, Puerto Rico, and Canada who applied online or by phone for store positions with Gap, Old Navy, Banana Republic, and Outlet stores, between July 2006 and June 2007.

8. Defendant's failure to maintain reasonable and adequate security procedures to protect against the theft of the job applicants' personal information has, *inter alia*, put Plaintiff and other Class members at an increased risk of becoming victims of identity theft crimes. As a result, Plaintiff and the Class seek injunctive relief and any other such relief as the Court may award.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because Plaintiff is of diverse citizenship from Defendant; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds $5,000,000, excluding interest and costs. This Court has personal jurisdiction over the parties because Defendant is a resident of this state, conducts substantial business in this state, has had systematic and continuous contacts with this state, and has agents and representatives that can be found in this state.

10. Venue is appropriate under the authority of 28 U.S.C. § 1391(b). Defendant resides in this District and a substantial part of the challenged actions of Defendant took place in this District.

FACTUAL ALLEGATIONS

Background of the Company

11. Gap operates approximately 3,131 retail and outlet stores throughout the United States and overseas under several different brands: Gap, Old Navy, Banana Republic, and Piperlime.

12. As of February 3, 2007, Gap had a work force of approximately 154,000 employees, which includes a combination of part-time and full-time employees.

Standard Business Practices for Ensuring Information Safety

13. Federal and state legislatures have passed a number of laws in recent years to ensure companies protect the security of sensitive personal information in the company's files. These

laws include requirements for the handling of personal information by financial institutions[1] and also impose proactive obligations on companies to maintain reasonable security measures to protect the personal information of individuals.[2] Specifically, the California legislature has passed a law aimed at protecting the proliferation of the social security numbers of individuals.[3]

14. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"), attached hereto as Exhibit A. In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a. Keep inventory of all computers and laptops where the company stores sensitive data;

b. Do not collect personally identifying information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c. Use social security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d. Encrypt the personal information particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;

---

[1] The Gramm-Leach-Bliley Act, enacted on November 12, 1999, requires the FTC and other government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions. The regulations required all covered businesses to comply with the Act by July 1, 2001.

[2] Cal Civ. Code § 17980.80 *et seq.* obligates companies that possess personal information to take all reasonable steps to destroy the personal information no longer needed by the business, notify residents whose unencrypted information has been acquired in an unauthorized manner, and to implement reasonable security measures.

[3] Cal. Civ Code. § 1798.85(3) prohibits any company from requiring a person to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

e. Do not store sensitive computer data on any computer with an Internet connection unless it is essential for conducting the business;

f. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

g. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

15. In addition, the FTC Report states a number of guidelines concerning the use of laptops in storing personal information. As the FTC Report states:

a. Restrict the use of laptops to employees who need them to perform their jobs;

b. Assess whether sensitive personal information needs to be stored on a laptop, and if not, delete the information with a "wiping" program overwriting the data on the laptop;

c. Consider allowing laptop users only to access sensitive information but not to store the information on their laptops;

d. Require employees to store laptops in a secure place; and

e. Encrypt any sensitive data contained on a laptop and configure the data so users cannot download any software or change security settings without approval from Information Technology specialists.

16. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

17. The California Department of Consumer Affairs' Office of Privacy Protection published a similar set of guidelines in February 2007 report entitled "Recommendation Practices of Notice of Security Breach Involving Personal Information" ("California privacy report"), attached hereto as Exhibit B. The California Privacy report states guidelines similar to those found in the FTC Report, including one for businesses to encrypt higher-risk personal information when they are contained in portable computers and devices.

18. Thefts of portable devices containing personal information have occurred with some frequency in recent years. Various members of the news media have questioned the safety precautions used by companies to protect such personal information. As the San Francisco Chronicle reported on September 29, 2007:

> The increasing frequency of these thefts has raised questions about why companies and government agencies keep sensitive personal information on laptops and other portable devices. Many security experts say that such information should be stored only on secure centralized servers.

19. A September 28, 2007 article from CNNMoney.com quotes David Perry, a data security expert with a computer software company, Trend Micro. In the article, Perry specifically questioned Gap's failure to protect the personal information of its job applicants. As Perry stated:

> [W]hy is this kind of data on a laptop? And if it was on a laptop, it should certainly have been encrypted... This is just one of the many number of incidents where the value of the stolen property is no longer the computer itself but the information that's on it... Even though Gap says it believes that the data wasn't the target of the theft, whoever has the laptop now knows what's on it... That's a big concern to those job applicants and to Gap if that information is misused.

20. As the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report"), more than 570 breaches involving theft of personal identifiers such as social security numbers were reported by the news media from January 2005 through January 2006. As the GAO Report states, these data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers." A number of these breaches have occurred at retailers.

21. These data breaches can lead to identity theft. As the GAO Report has stated, "identity theft" is a broad term encompassing various types of criminal activities. Generally, identity theft occurs when a person's identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud. The Federal Trade Commission ("FTC") has stated that identity theft has been

a serious problem in recent years, with approximately 9 million Americans as the victims of identity theft each year.

22. The GAO Report stated that identity thieves can use identifying data such as social security numbers to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating.

23. In addition, the GAO states that victims of identity theft will face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

The Job Application Process

24. Job applicants to any of the different Gap brand stores may fill out an in-person application, apply over the telephone, or apply online.

25. During the online application process, Gap informs the applicant of the following "Privacy Statement":

> Vangent has adopted the following Privacy Policy.[4] We provide and support Gap Inc.'s recruitment system that you are accessing. We use reasonable precautions to protect your personal information from unauthorized use, access, disclosure, alteration or destruction. We do not release any of your information with any party other than Gap Inc., unless directed by Gap Inc. or legally mandated to do so. Gap Inc. may require that your application information be given to a third party provider for the purposes of performing background checks and/or pursuing Work Opportunity Tax Credits.

https://gapinc.reidsystems.com/US/start.htm?lang=01&ctry=US (last accessed on November 5, 2007).

26. Throughout the online application, Gap requires the job applicant to provide a large amount of personal identifying information, including the applicant's social security number, birthdate, address, and phone number.

---

[4] Vangent is one of the vendors employed by Gap to manage its job applicant data. Gap has failed to identify which third party vendor owned the stolen laptops, and it is not known at this time whether Vangent is the third party vendor at issue here.

27. Job applicants cannot complete the online job application process unless they provide their social security number. Gap's online website does not offer the option to use a password, personal identification number, or authentication device other than the applicant's social security number, to access the online job application.

28. Job applicants are also required to consent to a background check as part of the application. Gap states in its online application that a social security number is required to enter the online application process but that it is solely used for the purpose of obtaining the applicant's credit report.

29. In addition, Gap's online application prompts the applicant to provide various forms of personal information, including certain behavior and personality traits. The applicant cannot continue the online application process unless these questions are answered. Applicants are required to answer such questions as:

a. whether the applicant has been convicted of a felony or misdemeanor;

b. whether the applicant's family has received food stamps from the federal government; and

c. whether the applicant has ever had a "good reason for cheating a company out of some money."

30. Gap employs multiple third-party vendors to manage its job application process. These vendors have full access to all personal information provided through the job application process.

Plaintiff's Personal Information is Compromised

31. In late 2006, Plaintiff applied for a position with Old Navy through Gap's online application website. As part of the application process, Plaintiff was required to provide all of the aforementioned personal information to complete the application process. Among the information provided, Plaintiff provided his social security number, email, home address, and telephone number, as well as responses to other personal questions on the website. As with the other job applicants to the website, Gap informed Plaintiff through its Privacy Statement that it

would use all "reasonable precautions to protect [the applicant's] personal information from unauthorized use, access, disclosure, alteration or destruction."

32. On September 19, 2007, Gap learned that two laptop computers were stolen from the offices of one of the third-party vendors it employed to manage its job applicant data. The laptops contained the personal information of persons that had applied to Old Navy, Gap, Banana Republic, or its outlet stores by telephone or the internet from July 2006 to June 2007.

33. Encryption of computerized data is a standard business practice employed to make sensitive business information unreadable to anyone except those possessing a key or password. However, neither Gap nor its vendors encrypted any of the job applicants' personal information contained on the stolen laptops. Thus, any person in possession of one of the stolen computers could readily view the sensitive information without a password.

34. Plaintiff received a letter dated September 28, 2007, from Gap signed by Gap Chairman and CEO Glenn Murphy. The letter stated that Plaintiff's personal information was among those compromised in the theft of the laptop.

35. The letter stated that Gap did not believe Plaintiff's personal information was the target of the theft. For reasons not disclosed, the letter also indicated that Gap did not believe personal information had been "accessed or used improperly." However, it is unexplained how Gap would know that; such a statement creates a false sense of safety.

36. Gap offered to provide Plaintiff with twelve months of credit monitoring and fraud assistance without charge. The monitoring offered is the "Triple Advantage Credit Monitoring Plan" by Experian. Plaintiff has until January 31, 2008 to sign up for this coverage.

37. The year of credit monitoring and fraud assistance offered by Gap inadequately protects Plaintiff and the putative class from identity theft. One year is not nearly long enough to protect Plaintiff and the putative class from the effects of the security breach which has caused their personal information to fall into the hands of criminals.

38. The credit monitoring and fraud assistance is further weakened by forcing Plaintiff and the putative class to waive fundamental rights. Buried in the "Terms and Conditions" of the credit monitoring plan is a requirement that Plaintiff, and the putative class, must waive their

Constitutional rights to a jury trial should the credit monitoring service fail in its essential function. In short, the credit monitoring could fail, and Gap's potential and current employees could be victims of data theft, and there would effectively be no recourse against Experian. Pre-dispute binding mandatory arbitration has been the center of much controversy for its bias against consumers resulting in a recent report by Public Citizen titled "The Arbitration Trap" (found at http://www.citizen.org/documents/Final_wcover.pdf), as well as Congressional scrutiny in the presently pending Arbitration Fairness Act of 2007.

Gap Compromised the Personal Information of 800,000 Job Applicants

39. The stolen laptop contained the unencrypted personal information of approximately 800,000 people that applied online or by telephone to positions with Gap, Banana Republic, Old Navy, and Outlet Stores between July 2006 and June 2007. The vast majority of applicants whose personal information was compromised were applicants to Old Navy Stores.

40. Gap maintained the personal information of its job applicants for over a year, well beyond its usefulness, as express by Gap:

> This application will only be considered for 90 days. If you have not been hired within 90 days of completing the application and you wish to continue to be considered for employment, you must complete another application. It's only necessary to complete this application once every 90 days.

https://gapinc.reidsystems.com/US/start.htm?lang=01&ctry= (last accessed on November 8, 2007).

41. Among other information, the laptop contained the names, social security numbers, birthdates, addresses, and other personal identifying information of job applicants from the United States and Puerto Rico.

42. The laptop also included the personal information of applicants from Canada, but not the Social Insurance numbers of Canadian applicants. Gap has decided to not notify or send letters to Canadian job applicants whose information was compromised because of Gap's belief that this group is "not at a higher risk for identity theft."

43. Gap has not revealed the third-party vendor that lost the personal information of the 800,000 job applicants. Gap employs multiple vendors to manage the data collected from its job applicants.

CLASS ACTION ALLEGATIONS

44. Plaintiff brings this suit as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of himself and all other similarly situated persons as members of a Class initially defined as follows:

> All persons that have applied for a position with Gap Inc., Old Navy, Banana Republic, Piperlime, Outlet Stores, or any other relevant Gap brand store, through Gap's application process from July 1, 2006 to July 31, 2007, and whose personal information was compromised in a laptop theft from one or more of Gap's third party vendors.

45. Numerosity. The proposed class is sufficiently numerous, as more than 800,000 job applicants have had their personal information compromised. Class members are so numerous and dispersed throughout the United States that joinder of all members is impracticable. Class members, can be identified by, *inter alia*, records maintained by Defendant.

46. Common Questions of Fact and Law. Common questions of fact and law exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class, pursuant to Rule 23(b)(3). Among the questions of fact and law that that predominate over any individual issues are:

a. Whether Gap failed to exercise reasonable security measures to protect the personal information of Plaintiff and the Class;

b. Whether Gap's failure to protect the personal information of Plaintiff and the Class violated their legally protected privacy interest under the California Constitution;

c. Whether Plaintiff and the Class are at an increased risk of identity theft as a result of Gap's failure to protect the personal information of Plaintiff and the Class;

d. Whether Defendant owed the legal duties discussed herein to Plaintiff and the Class and whether Defendant breached these duties; and

e. Whether Plaintiff and members of the Class are entitled to the relief sought, including injunctive relief.

47. Typicality. Plaintiff's claims are typical of the claims of members of the Class because Plaintiff and the Class sustained damages arising out of Defendant's wrongful conduct as detailed herein. Specifically, Plaintiff's and Class members' claims arise from Gap's failure to install and maintain reasonable security measures to protect the personal information of Plaintiff and the Class.

48. Adequacy. Plaintiff will fairly and adequately protect the interests of Class members and has retained counsel competent and experienced in class action lawsuits. Plaintiff has no interests antagonistic to or in conflict with those of Class members and therefore is an adequate representatives for Class members.

49. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because the joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of an inconsistent and potentially conflicting adjudication of the claims asserted herein. There will be no difficulty in the management of this action as a class action.

50. Notice. Plaintiff will provide the individual notice and/or notice by publication to the Class to the extent required by the Federal Rules of Civil Procedure, due process considerations, and as approved by the Court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

51. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

52. Defendant owed Plaintiff and the Class a duty to protect their private personal information.

53. Defendant was aware of a standard or "best practice" in the industry when it came to protecting the private information of employees and applicants. Given the considerable news

coverage of similar data breaches in recent years, Gap was clearly aware of the need to protect the personal information of its job applicants.

54. Defendant breached this duty by failing to take adequate measures to safeguard this information and, upon information and belief, specifically failed to maintain reasonable security procedures and practices appropriate to protect the personal information of Plaintiff and the Class.

55. Defendant failed to adhere to a number of reasonable and appropriate business practices regarding the personal information of Plaintiff and the Class, including:

a. Failing to keep an adequate inventory of all laptops on which personal information is stored;

b. Requiring Plaintiff and the Class to use their social security numbers to access the website without requiring some other unique password or authentication code;

c. Storing the personal information of Plaintiff and the Class beyond the time necessary to process their job applications;

d. Failing to properly ensure that all personal information was encrypted; and

e. Allowing the personal information to be stored on portable laptop computers.

56. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and the Class have been harmed by the release for their personal information by putting them at an increased risk of identity theft.

COUNT II

BAILMENT

57. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

58. Plaintiff and the Class delivered and entrusted their personal information to Defendant for the sole purpose of applying for a position with one of Gap's stores.

59. During the time of bailment, Defendant owed Plaintiff and the Class a duty to safeguard this information properly and maintain reasonable security procedures and practices to protect such information. As alleged herein, Defendant breached this duty.

60. As a result of these breaches of duty, Plaintiff and the Class have been harmed as alleged herein.

COUNT III

VIOLATION OF CAL. BUS. AND PROF. CODE §§ 17200 *ET SEQ.*; CALIFORNIA UNFAIR COMPETITION ACT

61. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

62. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the personal information of Plaintiff and the Class, Defendant violated the provisions of Cal. Bus. and Prof. Code §§ 17200 *et seq.*

63. As a result of Defendant's practices, Plaintiff and the Class have suffered an injury-in-fact by being at an increased risk of identity theft. In addition, plaintiffs have lost property in the form of their personal information.

64. Defendant's violation of the laws of this state and of common law by the practices complained of herein constitutes an unlawful business practice within the meaning of Cal. Bus. and Prof. Code §§ 17200 *et seq*. Defendant's practices, as described herein, violate federal, state, statutory, regulatory, or industry standards as described above in Paragraphs 13 to 19, including, but not limited to, the California Constitutional Right to Privacy, and Cal. Civ. Code 1798.85.

65. Defendant's requirement to transmit social security numbers over the Internet and attendant failure to encrypt or otherwise maintain reasonable security measures over such information violates not only the unlawful prong of Cal. Bus. and Prof. Code §§ 17200 *et seq.* but also constitutes an independent violation of the "unfair" prong of section 17200 independent of the other causes of action asserted herein. Gap's failure to adopt reasonable practices in protecting personal information has placed the Plaintiffs and the Class at a higher risk of identity theft crimes. This harm sufficiently outweighs any of Gap's justifications or motives for its practice of collecting and storing such information, namely, to perform background checks and/or pursue Work Opportunity Tax Credits.

66. The injury to Plaintiff and the Class caused by Defendant's failure to install, adopt, and maintain reasonable security procedures is substantial. As a result, the personal information of Plaintiff and the Class has been substantially compromised, placing them at a significant risk of being victims of identity theft and other harm.

67. The conduct alleged herein is a "business practice" within the meaning of Cal. Bus. and Prof. Code §§ 17200 *et seq.*

68. As a result of Defendant's actions, Plaintiff and the Class are entitled to the following forms of injunctive relief by Gap:

a. Establishment, implementation, and maintenance of a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from or about employees and potential employees;

b. Providing for a reasonable method of protecting and securing the personal information of all job applicants;

c. Encrypting any personal information collected from all job applicants;

d. Cease using social security numbers as a requirement to access the online job application website unless a password or unique personal identification number of other authentication device is also required for access;

e. Obtaining, every two years for the next 10 years, an audit from a qualified, independent, third-party professional to ensure that Gap's security program, and its vendors, meets the standards set forth in (a) and engage in best industry practices with regard to applicant data in the future;

f. Establishment of a fund to cover uninsured identity theft loss that Plaintiff and the Class may incur as a result of the complained-of conduct; and

g. Upgrade the current Triple Advantage Monitoring Plan offered to Plaintiffs and the Class by increasing the amount of identity theft insurance to $50,000 and to a period of five years, providing online access and monitoring to the FICO scores

of Plaintiff and the Class, and providing Plaintiffs and the Class the ability to quickly lock and unlock their credit report online.

COUNT IV

VIOLATION OF CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY

69. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

70. Fundamental to privacy is the ability to control circulation of personal information. The proliferation of business records over which individuals have no control limits their ability to control their personal lives. Thus, personal privacy is threatened by the information-gathering capabilities and activities of private business as well when these businesses fail to conform to adequately safeguard such information.

71. By reason of the conduct alleged herein, and by failing to protect against the theft of personal information of Plaintiff and the Class, Defendants violated the California constitutional right of privacy of Plaintiff and the Class.

72. Plaintiff and the Class have a legally protected privacy interest in their birthdates, social security numbers, and other personal information. In addition, Plaintiff and Class members have a reasonable expectation of privacy in this information. Defendant's invasion of this privacy interest is serious in that it puts the Plaintiff and Class members at risk of identity theft and the potential for substantial costs and injury associated with various crimes of identity theft.

73. Thus, Plaintiff and Class members are entitled to damages as a result of the violation of their constitutional right to privacy.

COUNT V

Violation of Cal. Civ. Code § 1798.85

74. Plaintiff repeats and realleges the allegations contained in each of the paragraphs of this complaint as if fully set forth herein.

75. By requiring Plaintiff and Class members to use social security numbers to enter the application process without also requiring a unique personal identification number or other authentication device, Defendant has violated Cal. Civ. Code § 1798.85.

76. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 1798.85, Plaintiff and the Class have been harmed as alleged herein. Plaintiff and Class members are entitled to damages as a result of the violation of Cal Civ. Code § 1798.85.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment on behalf of himself and those similarly situated as follows:

A. For an order certifying the proposed Class herein under Federal Rule of Civil Procedure 23(a) and (b)(3) and appointing Plaintiff and Plaintiff's counsel of record to represent said Class;

B. Awarding Plaintiff and Class members compensatory damages against Defendant in an amount to be determined at trial, together with prejudgment interest at the maximum rate allowable by law;

C. Grant all appropriate injunctive relief under Cal. Bus. and Prof. Code §§ 17200 *et seq.* as stated in Paragraph 38 above;

D. Grant all appropriate relief under Cal. Civ. Code § 1798.85;

E. Awarding Plaintiff and Class members the reasonable costs and expenses of suit, including attorneys' fees, filing fees; and

F. Grant additional legal or equitable relief as this Court may find just and proper.

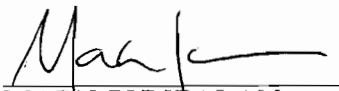
JURY TRIAL DEMANDED

Plaintiff demands a trial by jury.

Dated: November 13, 2007

Respectfully submitted,

FINKELSTEIN THOMPSON LLP



MARK PUNZALAN

Christine Pedigo Bartholomew
100 Bush Street, Suite 1450
San Francisco, CA 94104
Telephone: 415.398.8700
Facsimile: 415.398.8704

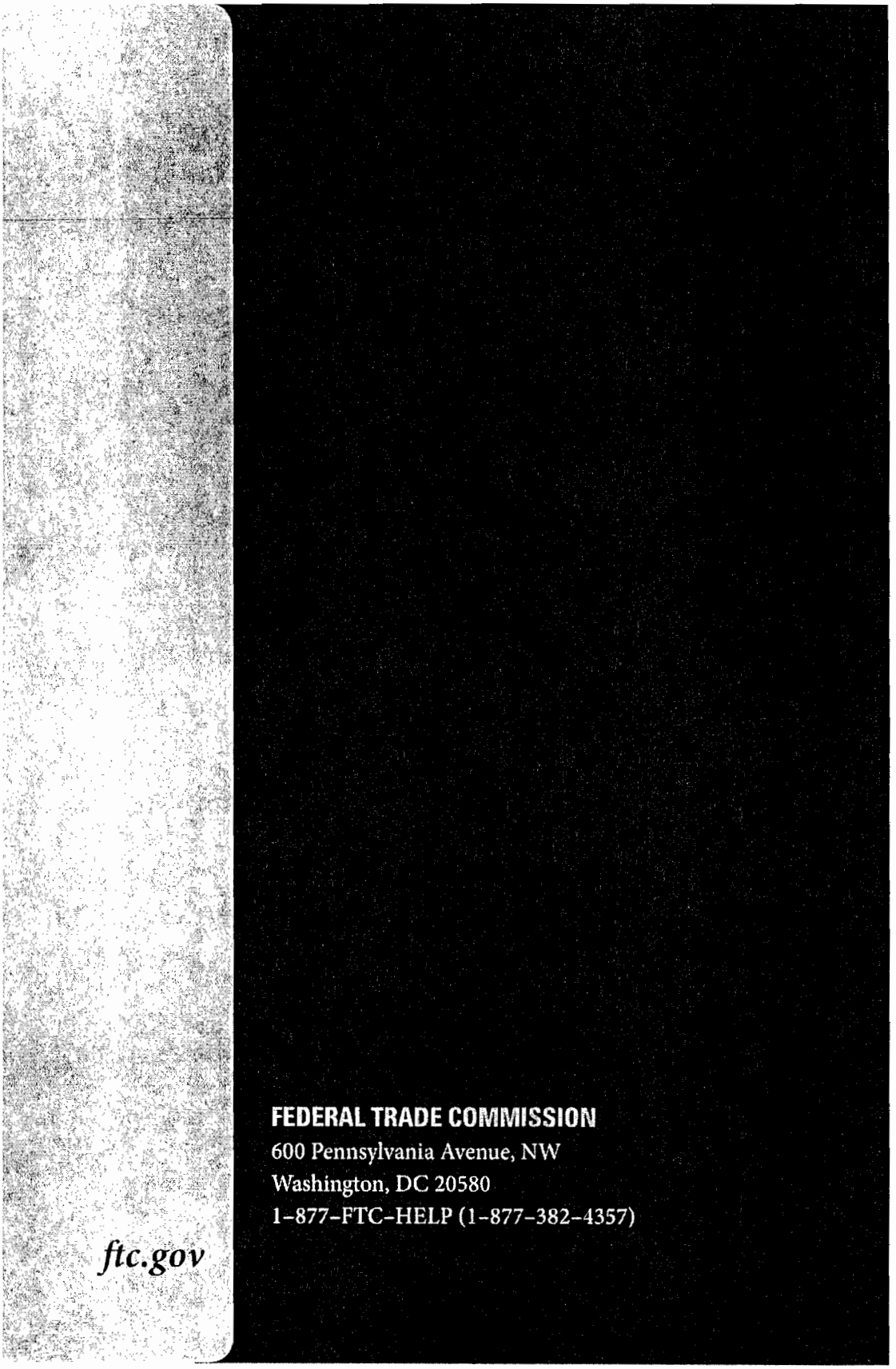
Mila F. Bartos
Tracy Rezvani
Karen J. Marcus
FINKELSTEIN THOMPSON LLP
1050 30th Street, NW
Washington, D.C. 20007
Telephone: 202.337.8000
Facsimile: 202.337.8090

Of Counsel
Ben Barnow
Barnow and Associates P.C.
One N. LaSalle Street
Suite 4600
Chicago, IL 60602

EXHIBIT A

Protecting PERSONAL INFORMATION
A Guide for Business

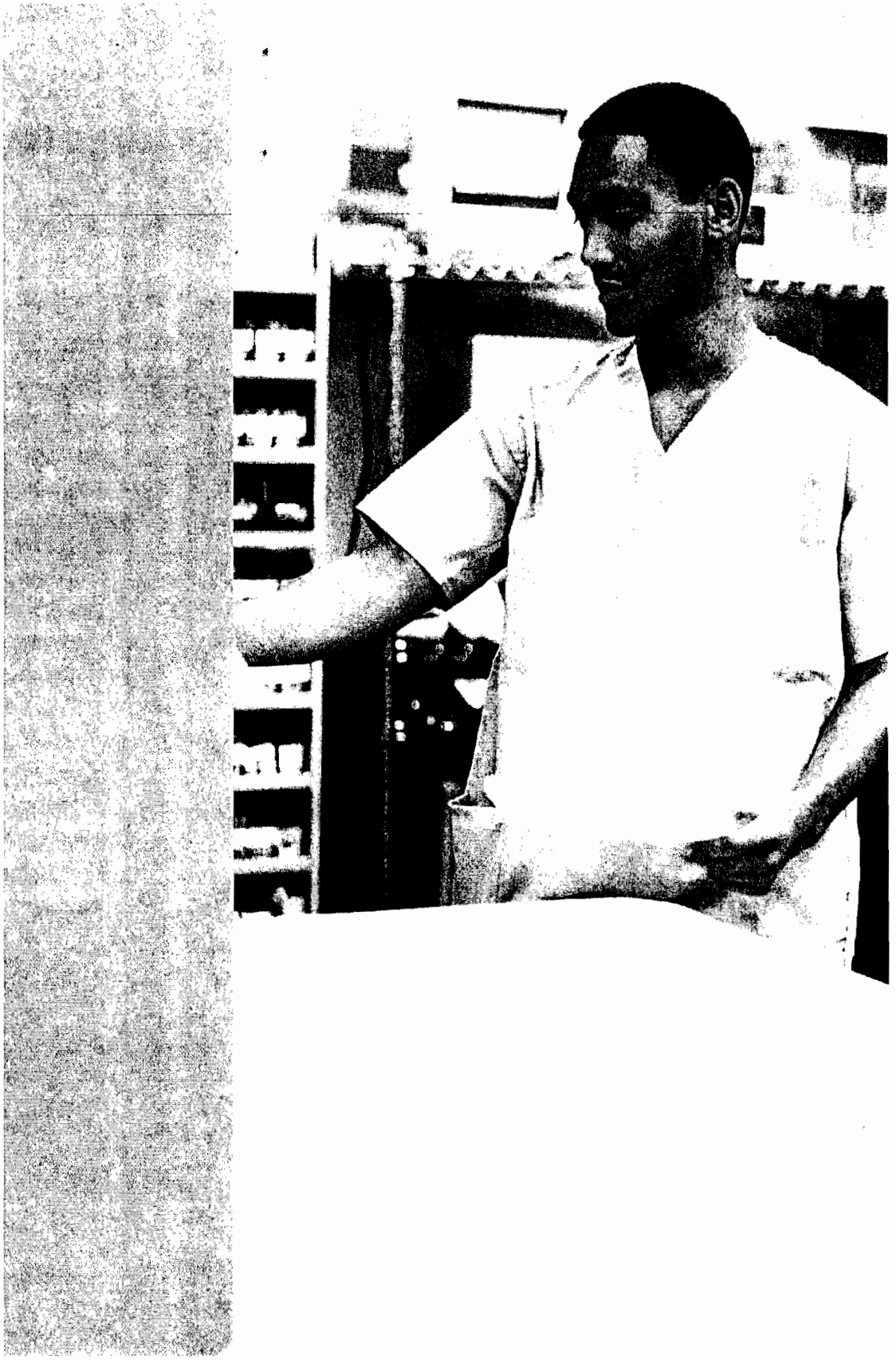
FEDERAL TRADE COMMISSION


FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357)
ftc.gov

PROTECTING PERSONAL INFORMATION
A Guide for Business

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.



A sound data security plan is built on **5 key principles:**

1. **Take stock.** Know what personal information you have in your files and on your computers.

2. **Scale down.** Keep only what you need for your business.

3. **Lock it.** Protect the information that you keep.

4. **Pitch it.** Properly dispose of what you no longer need.

5. **Plan ahead.** Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up—and where changes are necessary.

Know what personal information you have in your files and on your computers.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

- Inventory all computers, laptops, flash drives, disks, home computers, and other equipment to find out where your company stores sensitive data. Also inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember: your business receives personal information in a number of ways—through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, and cell phones? No inventory is complete until you check everywhere sensitive data might be stored.
- Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:

- ***Who sends sensitive personal information to your business.*** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Other businesses?
- ***How your business receives personal information.*** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?
- ***What kind of information you collect at each entry point.*** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
- ***Where you keep the information you collect at each entry point.*** Is it in a central computer database? On individual laptops? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?
- ***Who has—or could have—access to the information.*** Which of your employees has permission to access the information? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors operating your call center?

Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft.

SECURITY CHECK

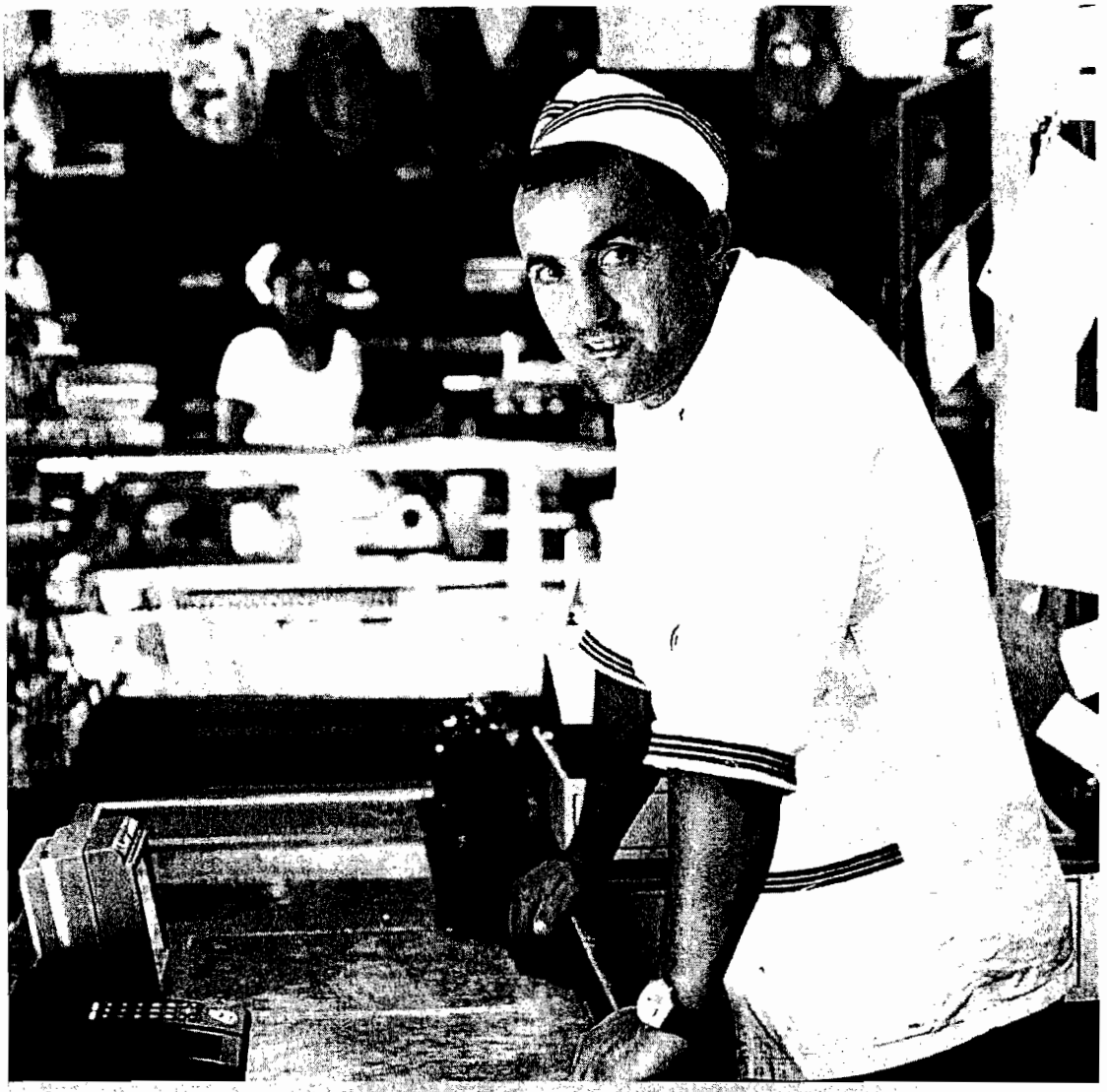
Question:

Are there laws that require my company to keep sensitive data secure?

Answer:

Yes. While you're taking stock of the data in your files, take stock of the law, too. Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit ***www.ftc.gov/privacy***.



Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes—like reporting employee taxes. Don't use Social Security numbers unnecessarily—for example, as an employee or customer identification number, or because you've always done it.

SECURITY CHECK

Question:

We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collected from the magnetic stripe on their credit cards. Could this practice put their information at risk?

Answer:

Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not in your system, it can't be stolen by hackers. It's as simple as that.

- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft.
- Check the default settings on your software that reads customers' credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently. Change the default setting to make sure you're not inadvertently keeping information you don't need.
- If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it.

Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

PHYSICAL SECURITY

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.

- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.

ELECTRONIC SECURITY

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the field.

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information. These may include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, and wireless devices like inventory scanners or cell phones.

- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
- Don't store sensitive consumer data on any computer with an Internet connection unless it's essential for conducting your business.
- Encrypt sensitive information that you send to third parties over public networks (like the Internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.
- Check expert websites (such as ***www.sans.org***) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.
- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

SECURITY CHECK

Question:

We encrypt financial data customers submit on our website. But once we receive it, we decrypt it and email it over the Internet to our branch offices in regular text. Is there a safer practice?

Answer:

Yes. Regular email is not a secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or ID thieves.

- Pay particular attention to the security of your web applications—the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack," a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available from a variety of sources.

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords—like common dictionary words—can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee's user name and password to be different, and require frequent changes in passwords.
- Explain to employees why it's against company policy to share their passwords or post them near their workstations.
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Lock out users who don't enter the correct password within a designated number of log-on attempts.

SECURITY CHECK

Question:

Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?

Answer:

Yes. Hackers will first try words like "password," your company name, the software's default password, and other easy-to-guess choices. They'll also use programs that run through common English words and dates. To make it harder for them to crack your system, select strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers. And change passwords often.

- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.
- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email. Unencrypted email is not a secure way to transmit any information.

- Restrict the use of laptops to those employees who need them to perform their jobs.
- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop. Deleting files using standard keyboard commands isn't sufficient because data may remain on the laptop's hard drive. Wiping programs are available at most office supply stores.
- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees' desks.

- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer.
- If a laptop contains sensitive data, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialists. Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.
- Train employees to be mindful of security when they're on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.

- Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
- Determine whether you should install a "border" firewall where your network connects to the Internet. A border firewall separates your network from the Internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set "access controls"—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.
- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

- Determine if you use wireless devices like inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.
- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.
- Better still, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called "spoofing"—impersonating one of your computers to get access to your network.
- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
- Have in place and implement a breach response plan. See pages 22–23 for more information.

EMPLOYEE TRAINING

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

Check references or do background checks before hiring employees who will have access to sensitive data.

Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties. Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.

Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know."

Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

SECURITY CHECK

Question:

I'm not really a "tech" type. Are there steps our computer people can take to protect our system from common hack attacks?

Answer:

Yes. There are relatively simple fixes to protect your computers from some of the most common vulnerabilities. For example, a threat called an "SQL injection attack" can give fraudsters access to sensitive data on your system, but can be thwarted with a simple change to your computer. Bookmark the websites of groups like the Open Web Application Security Project, ***www.owasp.org***, or SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities, ***www.sans.org/top20***, for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities.

Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don't attend, consider blocking their access to the network.

Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an offsite location.
- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.
- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.
- For computer security tips, tutorials, and quizzes for everyone on your staff, visit ***www.OnGuardOnline.gov***.

SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

Your company's security practices depend on the people who implement them, including contractors and service providers.

- Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company's data security practices and compare their standards to yours. If possible, visit their facilities.
- Address security issues for the type of data your service providers handle in your contract with them.
- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

Properly dispose of what you no longer need.

What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

SECURITY CHECK

Question:

My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications, we're careful to throw them away. Is that sufficient?

Answer:

No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

Effectively dispose of paper records by shredding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.

When disposing of old computers and portable storage devices, use wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.

Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.

If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? New Rule Tells How* at ***www.ftc.gov/privacy*** (click on Credit Reporting, Business Guidance).

Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have a plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.
- If a computer is compromised, disconnect it immediately from the Internet.

SECURITY CHECK

Question:

I own a small business. Aren't these precautions going to cost me a mint to implement?

Answer:

No. There's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff, etc.—will cost you next to nothing and you'll find free or low-cost security tools at non-profit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach.

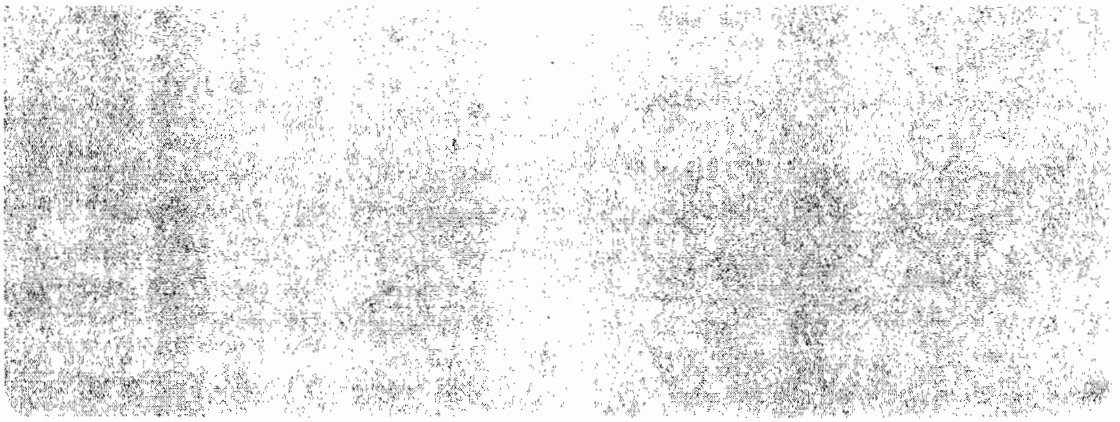
Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.

Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

ADDITIONAL RESOURCES

These websites and publications have more information on securing sensitive data:

- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center
  www.csrc.nist.gov
- NIST's Risk Management Guide for Information Technology Systems
  www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Department of Homeland Security's National Strategy to Secure Cyberspace
  www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities
  www.sans.org/top20
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov
- Carnegie Mellon Software Engineering Institute's CERT Coordination Center
  www.cert.org/other_sources
- Center for Internet Security (CIS)
  www.cisecurity.org
- The Open Web Application Security Project
  www.owasp.org
- Institute for Security Technology Studies
  www.ists.dartmouth.edu
- OnGuard Online
  www.OnGuardOnline.gov



The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free 1–877–FTC-HELP (1–877–382–4357); TTY: 1–866–653–4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and 10 Regional Fairness Boards collect comments from small business about federal enforcement actions. Each year, the Ombudsman evaluates enforcement activities and rates each agency's responsiveness to small business. To comment on FTC actions, call 1–888–734–3247.

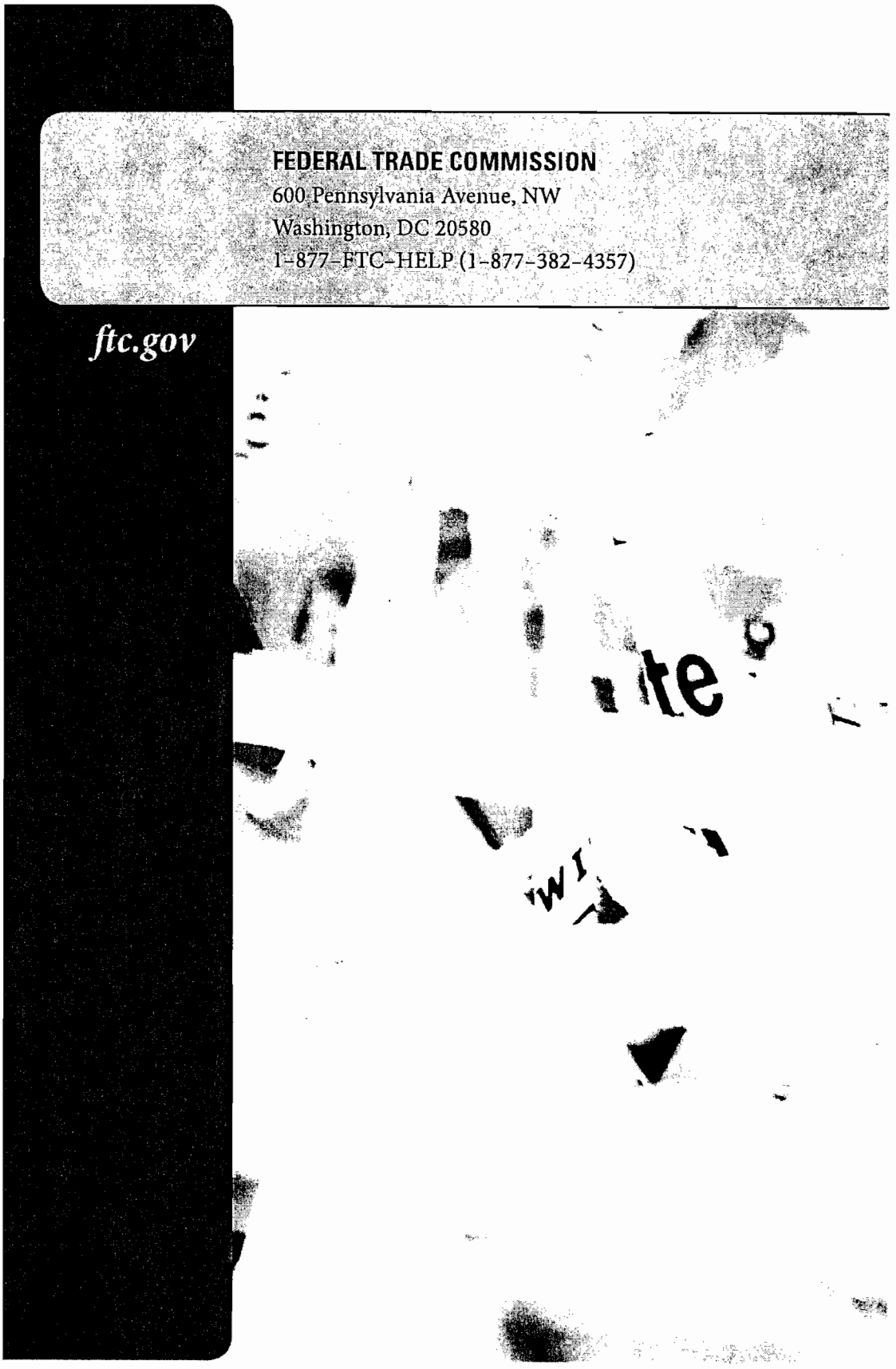

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357)
ftc.gov

EXHIBIT B

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

OFFICE OF
Privacy
Protection

Recommended Practices on Notice of Security Breach Involving Personal Information

February 2007

October 2003
Rev. April 2006
Rev. February 2007

California Office of Privacy Protection
www.privacy.ca.gov
866-785-9663

Contents

Introduction

Identity Theft

Identity theft has been called the crime of the 21st century, favored, according to law enforcement, for its low risks and high rewards. Not only do identity theft victims have to spend money out of pocket to clear up their records, but they also must devote their time – up to hundreds of hours in some cases – to doing so. In the meantime, victims may be unjustly harassed by debt collectors, denied credit or employment opportunities; they may lose their cars or their homes, or be repeatedly arrested for crimes they did not commit.

The incidence of identity theft seems to have become relatively stable in recent years. According to major nationwide surveys, around nine million Americans were victims of identity theft each year between 2003 and 2005.[1] If the same rate of about 4% of adults is applied to California, then over a million Californians become victims of identity theft in a year.

The costs of the crime are significant. Studies have estimated the average victim's out-of-pocket expenses at $422 to $851, and the average time spent clearing up the situation at 40 to 330 hours.[2] The most recent study put the total cost to business and victims at $56.6 billion in 2005.[3]

Precisely how most identity theft occurs and the role of information security breaches is not clear. The nationwide surveys found that half of victims do not know how their personal information was acquired by the thief.[4] One academic study of identity theft cases found that in over half of the crimes, insiders in organizations were involved.[5]

Information Security

Security has always been an essential component of information privacy. It is one of the basic principles of fair information practice: Organizations that collect or manage individuals' personal information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification, or destruction.[6]

Implementing an effective information security program is essential for an organization to fulfill its responsibilities towards the individuals who entrust it with their personal information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of an information security breach and the resultant cost to an organization's reputation and finances.

Many organizations in the United States are legally required to protect the security of personal information. The two major federal laws on privacy enacted in recent years - the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act - include security regulations that apply to a broad range of financial institutions and health care organizations.[7] A California law also requires businesses to use reasonable and appropriate security measures to protect specified personal information of California residents.[8] Another California law makes a similar requirement of state government agencies.[9]

Security Breach Notification

One of the most significant privacy laws in recent years is the California law intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crime's impact.

Since the California law requiring notifica-

tion of security breaches involving personal information took effect in 2003, news reports of breaches have brought the issue of information security to public attention. Notifying affected individuals in such cases has become a fairly standard practice, and several states have enacted notification laws based on California's.

The breach notice law has done more than give individuals notice; it has also resulted in improved privacy and security practices in many organizations. While the law does not require entities experiencing a breach to notify the California Office of Privacy Protection, many individuals, companies, and agencies have contacted the Office with questions about notification. In an effort to identify and spread best practices, the Office has studied these breach notifications and has synthesized many lessons learned from them.

One lesson is made clear by the significant share of breaches resulting from lost or stolen laptops and other portable devices, about 53% of the Office's sample. Organizations have begun to pay more attention to protecting personal information on portable devices. Some organizations are doing this by using encryption. Others have adopted new procedures to safeguard the information, such as cabling PCs to desks, not allowing the downloading of Social Security numbers from mainframes onto PCs or laptops, and tightly restricting the number of people who are permitted to carry sensitive personal information on portable devices.

Another lesson is the ubiquity of Social Security numbers in databases and other records. Fully 85% of the breaches in the Office of Privacy Protection's sample involved Social Security numbers. Individuals face the greatest risk of serious identity theft problems when their Social Security numbers fall into the wrong hands. Recovering from these types of identity theft can take hundreds of hours and thousands of dollars, making early discovery critical.

Some organizations that have experienced breaches of Social Security numbers have revised their data retention policies. After a breach that exposed 15-year-old data, a university reviewed their policies and decided to shorten the retention period for certain information, including Social Security numbers, on applicants who were not admitted.

Others have reconsidered their collection of the sensitive personal information in the first place. One blood bank which, like several others with mobile operations, had a laptop stolen, changed its policy of collecting Social Security numbers and decided to rely instead on the donor numbers that they were already using.

The California Office of Privacy Protection's Recommended Practices

California law obligates the California Office of Privacy Protection to protect the privacy of individuals' personal information by "identifying consumer problems in the privacy area and facilitating [the] development of fair information practices."[10] One of the ways that the Office is directed to do this is by making "recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[11]

The recommendations offered here are neither regulations, nor mandates, nor legal opinions. Rather, they are a contribution to the development of "best practices" for businesses and other organizations to follow in managing personal information in ways that promote and protect individual privacy interests. If you have questions about the recommendations, you may contact the Office at 866-785-9663.

In developing the recommendations, the Office received consultation and advice from an advisory group made up of representatives of the financial, health care, retail, technology and information industries, state government agencies, law enforcement, and consumer privacy advocates.[12] The group members' contributions were very helpful and are greatly appreciated.

California Law on Notice of Security Breach

California Civil Code Section 1798.29 applies to government agencies and Sections 1798.82 to 1798.84 apply to any person or business doing business in California. The full text of the law is attached as Appendix 3. The main provisions are summarized below.

Security Breach

- Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

Type of Information

- Unencrypted computerized data including certain personal information.
- Personal information that triggers the notice requirement is name (first name or initial and last name) plus any of the following:
  - Social Security number,
  - Driver's license or California Identification Card number, OR
  - Financial account number, credit or debit card number (along with any PIN or other access code where required for access to account).

Whom to Notify

- Notice must be given to any data subjects who are California residents.

When to Notify

- Timing: "in the most expedient time possible and without unreasonable delay." Time may be allowed for the following:
  - Legitimate needs of law enforcement if notification would impede a criminal investigation.
  - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

How to Notify

- Notice may be provided in writing, electronically (as consistent with provisions on electronic records and signatures per 15 U.S. Code 7001), or by substitute notice.
- Substitute notice may be used if the cost of providing individual notice is more than $250,000, more than 500,000 people would have to be notified, or the organization does not have sufficent contact information for those affected.
- Substitute notice means all of the following:
  - E-mail when the e-mail address is available, AND
  - Conspicuous posting on Web site, AND
  - Notification of major statewide media.
- Alternatively, the business or agency may use its own notification procedures as part of an information security policy for personal information, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Recommended Practices

The California Office of Privacy Protection's recommendations are intended to assist organizations in supplementing their information security programs. The recommendations are not regulations and are not binding. Nor are they limited to the scope of the California law on notice of security breach, but rather they represent a broader approach and a higher standard.

These "best practices" recommendations can serve as guidelines for organizations, to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. Unlike many best practices sets, however, these recommendations do not contain all the practices that should be observed. Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their own situation to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

Our practice recommendations are presented in three parts: Part I - Protection and Prevention, Part II - Preparation for Notification, and Part III - Notification. While the California law on notice of security breach applies to unencrypted "computerized data," we recommend applying these practices to records in any media, including paper records.

Definitions

The following are definitions of key terms used in these recommended practices. (Note that the terms are not used in the statute.)

Notice-triggering information: As provided in California law, this is unencrypted, computerized first name or initial and last name plus any of the following: Social Security number, driver's license number, California Identification Card number, or financial account number, credit or debit card number, in combination with any code or password permitting access to an individual's financial account where such a code or password is required.

Higher-risk personal information: This is not only the notice-triggering information that could subject an individual to identity theft, but also health information, other financial information, and other personal information the disclosure of which would violate the privacy of individuals.

Data owner. The individual or organization with primary responsibility for determining the purpose and function of a record system.

Data custodian: The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of the record system.

Part I: Protection and Prevention

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multi-layered program to protect personal information from unauthorized access.[13] An organization should protect the confidentiality of personal information whether it pertains to customers, employees or others. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices.

1. Collect the minimum amount of personal information necessary to accomplish your business purposes, and retain it for the minimum time necessary.

2. Inventory records systems, critical computing systems, and storage media to identify those containing personal information.

- Include laptops and portable devices used to store personal information.

3. Classify personal information in records systems according to senstivity.

- Identify notice-triggering and other higher-risk personal information.

4. Use appropriate physical and technological security safeguards to protect personal information, particularly higher-risk information, in paper as well as electronic records.

- Authorize employees to have access to only the specific categories of personal information their job responsibilities require.
- Where possible, use technological means to restrict internal access to specific categories of personal information.
- Monitor employee access to higher-risk personal information.
- Remove access privileges of former employees and contractors immediately.

5. Pay particular attention to protecting higher-risk personal information on laptops and other portable computers and storage devices.

- Restrict the number of people who are permitted to carry such information on portable devices.
- Consider procedures such as cabling PCs to desks or prohibiting the downloading of higher-risk personal information from servers onto PCs or laptops.
- Use encryption to protect higher-risk personal information on portable computers and devices.[14]

6. Promote awareness of security and privacy policies and procedures through ongoing employee training and communications.

- Monitor employee compliance with policies and procedures.
- Include all new, temporary, and contract employees in security and privacy training and monitoring.
- Impose penalties for violation of security and privacy policies and procedures.

7. Require service providers and business partners who handle personal information on behalf of your organization to follow your security policies and procedures.

- Make privacy and security obligations of third parties enforceable by contract.[15]
- Monitor and enforce third-party compliance with your privacy and security policies and procedures.

8. Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.

- Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches.

9. Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information.

- Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.[16]

10. Dispose of records and equipment containing personal information in a secure manner.

- Shred paper records with a cross-cut shredder and use a program to "wipe" and overwrite the data on hard drives.[17]

11. Review your security plan at least annually or whenever there is a material change in business practices that may reasonably implicate the security of personal information.

- For example, if an organization decides to outsource functions that use personal information, such as using a call center, the plans should be revisited to take the new third parties into account.

Part II: Preparation for Notification

An information security program should contain an incident response plan, which addresses security incidents including unauthorized access to or acquisition of higher-risk personal information.[18] To ensure timely notice to affected individuals, the following practices are among those that should be included in an incident response plan.

1. Adopt written procedures for internal notification of security incidents that may involve unauthorized access to higher-risk personal information.

2. Designate one individual as responsible for coordinating your internal notification procedures.

3. Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your incident response plan.

- Collect 24/7 contact numbers for incident response team and provide to team members.
- Make sure that all employees and contractors can recognize a potential breach and know where to report it.

4. Define key terms in your incident response plan and identify responsible individuals.

5. Plan for and use measures to contain, control and correct any security incident that may involve higher-risk personal information.

6. Require the data custodian or others who detect an information security incident to immediately notify the data owner upon the detection of any security incident that may involve unauthorized access to the record system.

7. Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities.

- Appropriate law enforcement agencies may include California's regional high-tech crimes task forces, the Federal Bureau of Investigation, the U.S. Secret Service, and the local police or sheriff's

department. See Appendix 4 for contact information.

8. Consider suggestions from law enforcement with expertise in investigating high-technology crimes for inclusion in your incident response plan.[19]

9. If you plan to notify affected individuals by e-mail, get the individuals' prior consent to the use of e-mail for that purpose.

- See the consent procedures in the federal Electronic Signature Act.[20]

10. Adopt written procedures for notification of individuals whose unencrypted notice-triggering personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.

- Include unauthorized acquisition of computer printouts and other paper records containing notice-triggering personal information in your notification procedures.

11. Document response actions taken on an incident. This will be useful to your organization and to law enforcement, if involved.

- At the conclusion of an incident, review events and actions and make any indicated changes in your technology and response plan.

12. Review your incident response plan at least annually or whenever there is a material change in your business practices.

Part III: Notification

Openness or transparency is another basic privacy principle. An organization that collects or manages personal information should be open about its information policies and practices. This responsibility includes informing individuals about incidents such as security breaches that have caused their unencrypted personal information to be acquired by unauthorized persons. The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.

To ensure giving timely and helpful notice to affected individuals, the following practices are recommended.

Acquisition

In determining whether unencrypted notice-triggering information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been downloaded or copied.
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Timing of Notification

Notify affected individuals in the most expedient time possible after the discovery of an incident involving unauthorized access to notice-triggering information.

1. Take necessary steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach.
2. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals

within 10 business days.

- Do this unless law enforcement authorities tell you that providing notice at that time would impede their investigation.

Contacting Law Enforcement

If you believe that the incident may involve illegal activities, report it to appropriate law enforcement agencies.

1. In contacting law enforcement, inform the law enforcement official in charge of the investigation that you intend to notify affected individuals within 10 business days.
2. If the law enforcement official in charge tells you that giving notice within that time period would impede the criminal investigation:
   - Ask the official to inform you as soon as you can notify the affected individuals without impeding the criminal investigation.
   - Be prepared to send the notices immediately upon being so informed.
   - It should not be necessary for a law enforcement agency to complete an investigation before notification can be given.

Whom to Notify

If your assessment leads you to reasonably believe that notice-triggering information was acquired by an unauthorized person, implement your notification plan.

1. Notify California residents whose notice-triggering information was acquired by an unauthorized person.
2. Notify affected individuals in situations involving unauthorized acquisition of notice-triggering information in any format, including computer printouts and other paper records.
3. Consider providing notice in breaches involving higher-risk personal information, even when it is not "notice-triggering" information under California law, if being notified would allow individuals to take action to protect themselves from possible harm.
4. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in the groups likely to have been affected, such as all whose information is stored in the files involved.
5. Avoid false positives. A false positive occurs when the required notice of a security breach is sent to individuals who should not receive it because their personal information was not acquired as part of the breach. Consider the following when identifying the group that will be notified.
   - Before sending individual notices, make reasonable efforts to include only those individuals whose notice-triggering information was acquired.
   - Implement procedures for determining who gets included in the notice and who does not. Check the mailing list before sending the notice to be sure it is not over-inclusive.
   - Document your process for determining inclusion in the group to be notified.

Contact Credit Reporting Agencies

A breach involving a large number of individuals can potentially have a significant impact on consumer reporting agencies and their ability to respond efficiently. High volumes of calls could impede access to the agencies. Be sure to contact the agencies before you send out notices in cases involving a large number of individuals—10,000 or more.

1. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason.

2. Organizations should contact the consumer credit reporting agencies as follows.
   - Experian: Send an e-mail to BusinessRecordVictimAssistance @Experian.com.
   - Equifax: Send an e-mail to businessrecordsecurity@equifax.com.
   - TransUnion: Send an e-mail to fvad@transunion.com, with "Database Compromise" as the subject.

Contents of Notice

Sample notice letters are attached as Appendix 2. Include the following information in your notice to affected individuals:

1. A general description of what happened.
2. The type of personal information that was involved: Social Security number, driver's license or state ID card number, bank acount number, credit card number, or other financial account number.
3. What you have done to protect the individual's personal information from further unauthorized acquisition.
4. What your organization will do to assist individuals, including providing your toll-free contact telephone number for more information and assistance.
5. Information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies.
6. Contact information for the California Office of Privacy Protection and/or the Federal Trade Commission for additional information on protection against identity theft.
   - California Office of Privacy Protection www.privacy.ca.gov
   - Federal Trade Commission www.consumer.gov/idtheft

Form and Style of Notice

Make the notice clear, conspicuous and helpful.

1. Use clear, simple language, guiding subheads, and plenty of white space in the layout.
2. Avoid jargon or technical language.
3. Avoid using a standardized format, which could result in making the public complacent about the process and thus undercut the purpose of the notice.

Means of Notification

Individually notify those affected whenever possible.

1. Send the notice by first-class mail.
2. As an alternative, notify by e-mail, if you normally communicate with the affected individuals by e-mail and you have received their prior consent to that form of notification.
3. If more than 500,000 individuals were affected, the cost of individual notification is more than $250,000, or you do not have adequate contact information on those affected, provide notice using public communication channels.
   - Post the notice conspicuously on your Web site, AND
   - Notify through major statewide media (television, radio, print), AND
   - Send the notice by e-mail to any affected party whose e-mail adddress you have.

Notes

[1]The Federal Trade Commission's, *Identity Theft Survey Report* of September 2003, is available on the FTC Web site at <www.ftc.gov/os/2003/09/synovatereport.pdf>. The Better Business Bureau sponsored similar nationwide surveys in 2004 and 2005. They can be found on the Javelin Strategy & Research Web site at <www.javelinstrategy.com/research>. Abbreviated versions of the BBB/Javelin surveys are available for free and the full survey reports may be purchased online.

[2]The 2005 BBB/Javelin survey cited above reported that the average victim spent $422 and 40 hours. A study by the Identity Theft Resource Center, *Identity Theft: The Aftermatch 2004*, found the average victim spent $851 and 330 hours. That report is available at <www.idtheftcenter.org>.

[3]See the 2005 BBB/Javelin survey cited above.

[4]The BBB/Javelin surveys reported that 53% of victims did not know how their information was obtained by the thief in 2005, and 46% did not know in 2004. The FTC survey reported that 47% did not know in 2003.

[5]"Identity Theft: Predator Profiles," Collins, J.M. and Hoffman, S.K. (2004). Available from Judith Collins, School of Criminal Justice, Michigan State University.

[6]This formulation of the security safeguards principle is from the Organisation for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

[7]The Gramm-Leach-Bliley Act, 15 USC 6801-6827, includes the Safeguards Rule, "Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information," 16 C.F.R. Part 314. The Health Insurance Portability and Accountability Act, PL 104-191, includes "Health Insurance Reform: Security Standards," 45 C.F.R. Parts 160, 162, and 164.

[8]California Civil Code Section 1798.81.5 requires companies that collect specified personal information (name plus Social Security number, driver's license or state ID number, financial account number, or medical information) on California residents to use reasonable and appropriate security safeguards to protect it. It also requires such companies to contractually obligate service providers to the same standards.

[9]California Civil Code Section 1798.21. The Information Practices Act, Civil Code Section 1798 et seq., imposes several specific responsibilities for protecting the security and confidentiality of records containing personal information.

[10]California Business and Professions Code section 350(a).

[11]California Business and Professions Code section 350(c).

[12]A list of the members of the advisory group is attached as Appendix 1.

[13]The internationally recognized information security standard is ISO/IEC 17799, a comprehensive set of controls comprising best practices in information security. For more information on the principles and practices of information security, see Appendix 5: Information Security Resources.

[14]The State of California has adopted a

policy requiring State agencies to encrypt "notice-triggering" and medical information on portable computing devices or portable storage media. See BL05-32, available at <www.dof.ca.gov>.

[15]See California Civil Code Section 1798.81.5.

[16]Effective May 26, 2002, the encryption standard approved for U.S. Government organizations and others to protect higher-risk information is FIPS 197. For more information, see <http://csrc.nist.gov/CryptoToolkit/aes/index.html#fips>.

[17]See Special Publication 800-88, *Guidelines for Media Sanitization*, published in February 2006 by the Computer Security Division of the National Institute of Standards and Technology, available at <http://csrc.nist.gov/publications/drafts.html>.

[18]ISO/IEC 17799, cited in note 13 above, includes practices related to responding to and reporting security incidents and malfunctions "as quickly as possible" (§ 6.3).

[19]See Appendix 4 for suggestions on computer security incident response from the California Highway Patrol's Computer Crimes Investigations Unit and the FBI's National Computer Crime Squad.

[20]15 U.S. Code Section 7001 contains the requirements for consumer disclosure and consent to electronic notification, as required by California Civil Code Sections 1798.29(g)(2) and 1798.82(g)(2).

Appendix 1: Advisory Group

Brent Barnhart
Senior Counsel
Kaiser Foundation Health Plan, Inc.

Camille Busette
Senior Policy Manager
Intuit

Dianne Carpenter
Senior Attorney
J.C. Penney Corporation
California Retailers Association

James Clark
Senior Vice President
Government Relations
California Bankers Association

Mari Frank
Attorney, Privacy Consultant, and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Roxanne Gould
Vice President, CA Public and Legislative Affairs
American Electronics Association

Chief Kevin Green
California Highway Patrol

Craig Grivette
Deputy Secretary
California Business, Transportation and Housing Agency

Tony Hadley
Vice President
Government Affairs
Experian

Gail Hillebrand
Senior Attorney
Consumers Union

Clark Kelso
Chief InformationOfficer
State of California

Barbara Lawler
Chief Privacy Officer
Hewlett-Packard

Fran Maier
Executive Director
TRUSTe

Dana Mitchell
Counsel to Rules Committee
California State Senate

Peter Neumann
Principal Scientist
Computer Science Lab
SRI International

Dr. Larry Ponemon
Chairman
Ponemon Institute

Debra Reiger
Information Security Officer
State of California

Tim Shea
Legal Counsel
California Franchise Tax Board

Scott Shipman
Privacy Counsel
eBay

Preston Taylor
Consultant to
Assemblyman Joseph Simitian
California State Assembly

Tracey Thomas
Identity Theft Resource Center

Tom Timmons
President & CEO, Spectrum Bank
California Independent Bankers

Appendix 2: Sample Notice Letters

SAMPLE LETTER 1
Data Acquired: Credit Card Number or Financial Account Number Only

Dear :

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, what type of personal information was involved, and what you are doing in response.*]

To protect yourself from the possibility of identity theft., we recommend that you immediately contact [*credit card or financial account issuer*] at [*phone number*] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask [*name of account issuer*] to give you a PIN or password. This will help control access to the account.

For more information on identity theft, we suggest that you visit the Web site of the California Office of Privacy Protection at www.privacy.ca.gov [or the Federal Trade Commission at www.consumer.gov/idtheft]. If there is anything [*name of your organization*] can do to assist you, please call [*toll-free phone number*].

[*Closing*]

SAMPLE LETTER 2
Data Acquired: Driver's License or California ID Card Number

Dear :

We are writing to you because of a recent security incident at [*name of organization*]. [*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

Since your Driver's License [*or California Identification Card*] number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free DMV Fraud Hotline at 866-658-5758 for additional information.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the California Office of Privacy Protection at www.privacy.ca.gov [or the Federal Trade Commission at www.consumer.gov/idtheft]. If there is anything [*name of your organization*] can do to assist you, please call [*toll-free phone number*].

[*Closing*]

SAMPLE LETTER 3
Data Acquired: Social Security Number

Dear :

We are writing to you because of a recent security incident at [*name of organization*]. [*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the California Office of Privacy Protection at www.privacy.ca.gov [or the Federal Trade Commission at www.consumer.gov/idtheft]. If there is anything [*name of your organization*] can do to assist you, please call [*toll-free phone number*].

[*Closing*]

Appendix 3: California Law on Notice of Security Breach

California Civil Code Sections 1798.29, 1798.82, and 1798.84

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed

two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic

records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.84. (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable. (b) Any customer injured by a violation of this title may institute a civil action to recover damages. (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(f) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Appendix 4: Reporting to Law Enforcement

Law Enforcement Contacts for Computer Crimes

California High Technology Theft and Apprehension Program
This program funds five regional task forces staffed by investigators from local, state and federal law enforcement agencies who have received specialized training in the investigation of high technology crime and identity theft investigations. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or is the target of a criminal act.

Sacramento Valley Hi-Tech Crimes Task Force
Telephone: 916-874-3002
www.sachitechcops.org

Southern California High Tech Task Force
Telephone: 562-347-2601

Northern California Computer Crimes Task Force
Telephone: 707-253-4500
www.nc3tf.org

Rapid Enforcement Allied Computer Team (REACT)
Telephone: 408-494-7186
http://reacttf.org

Computer and Technology Crime High-Tech Response Team (CATCH)
Telephone: 619-531-3660
http://www.catchteam.org/

FBI
Local Office: http://www.fbi.gov/contact/fo/fo.htm
National Computer Crime Squad
Telephone: 202-324-9164
E-mail: nccs@fbi.gov
www.emergency.com/fbi-nccs.htm

U.S. Secret Service
Local Office: www.treas.gov/usss/index.shtml
Cyber Threat/Network Incident Report: www.treas.gov/usss/net_intrusion_forms.shtml

Procedures the Computer User Should Institute Both Prior to Becoming a Computer Crime Victim and After a Violation Has Occurred

Guidance from the FBI National Computer Crime Squad
www.emergency.com/fbi-nccs.htm

- Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.
- Turn audit trails on.
- Consider keystroke level monitoring if adequate banner is displayed.
- Request trap and tracing from your local telephone company.
- Consider installing caller identification.
- Make backups of damaged or altered files.
- Maintain old backups to show the status of the original.
- Designate one person to secure potential evidence
- Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence. Evidence should be retained in a locked cabinet with access limited to one person.
- Keep a record of resources used to reestablish the system and locate the perpetrator.

Reporting a Computer Crime to Law Enforcement

Guidance from the California Highway Patrol Computer Crimes Investigation Unit
www.chp.ca.gov/html/computercrime.html

When reporting a computer crime be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).

- Operating System of the affected computer(s).
- Location of the affected computer(s).

Incident Response DOs and DON'Ts

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.
9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.
10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DON'Ts

1. Delete, move, or alter files on the affected systems.
2. Contact the suspected perpetrator.
3. Conduct a forensic analysis.

California Penal Code Definition of "Computer Crime"[1]

As defined by California Penal Code Section 502, subsection (c), a computer crime occurs when a person:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting docu-

mentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

[1]Other violations of California or federal law may also be involved in an incident of unauthorized acquisition of personal information. California laws that may be involved include identity theft (Penal Code § 530.5), theft (Penal Code § 484), or forgery (Penal Code § 470).

Appendix 5: Information Security Resources

CERT®, "Security Improvement Modules," available at < www.cert.org/security-improvement/index.html#practices >.

Federal Trade Commission, "Financial Institutions and Customer Data: Complying with the Safeguards Rule," available at <www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm >.

Federal Trade Commission, "Security Check: Reducing Risks to Your Computer Systems," available at < www.ftc.gov/bcp/conline/pubs/buspubs/security.htm >.

"Health Insurance Reform: Security Standards; Final Rule," 45 CFR Parts 160, 162 and 164, available at <www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>.

Internet Security Alliance, "Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices," (July 2002), available at <www.isalliance.org/news/requestform.cfm >.

ISO/IEC 17700:2005, Information Technology - Security Techniques - Code of Practice for Information Security Management, available at <www.iso.org>.

National Institute for Standards and Technology (NIST) Computer Security Resource Center, available at <www.csrc.nist.gov>.

Payment Card Industry Data Security Standard, available at <www.visa.ca/ais> and <https://sdp.mastercardintl.com>.

State Administrative Manual, Sections 4840-4845: Security and Risk Management, available at < sam.dgs.ca.gov/TOC/4800/default.htm >.

Arnold Schwarzenegger
Governor

Rosario Marin
Secretary
State and Consumer Services Agency

Charlene Zettel
Director
Department of Consumer Affairs

Joanne McNabb
Chief
California Office of Privacy Protection